



Department of Homeland Security Daily Open Source Infrastructure Report for 07 June 2006

Current
Nationwide
Threat Level is

ELEVATED
SIGNIFICANT RISK OF
TERRORIST ATTACKS

[For info click here](http://www.dhs.gov/)

<http://www.dhs.gov/>

Daily Highlights

- The Associated Press reports that with aluminum prices at an 18-year high, thieves are now targeting aluminum products, and experts say safety is at risk as items from light poles to highway guard rails are disappearing. (See item [1](#))
- The Associated Press reports laptop computers with personal information on 72,000 Ohio Medicaid recipients were stolen from Buckeye Community Health Plan, a private managed care agency in Columbus, Ohio. (See item [7](#))

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: [Energy](#); [Chemical Industry and Hazardous Materials](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation and Border Security](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information Technology and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [Commercial Facilities/Real Estate, Monument & Icons](#); [General](#); [DHS Daily Report Contact Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://www.esisac.com>]

1. *June 06, Associated Press* — **Metal thieves likely to turn to aluminum.** Thieves, stealing copper for years as prices have risen, have been mostly an expensive nuisance. Now they are targeting aluminum products, with experts saying safety is at risk as everything from light poles to highway guard rails are disappearing. "Aluminum prices are at an 18-year high," said Chuck Carr of the Institute for Scrap Recycling Industries. Highway guardrails and light rails have been stolen for years on the East Coast but "now it's everywhere," said Matt Haslett of Metro Metals Northwest. Officers are staging metals theft stings. Strong demand from Asia is driving the metals market, said Robin Adams of CRU Strategies. He contends the mining industry was

caught by surprise by demand and can't keep up with supplies of basic metals. The trend is likely to continue for a couple of years, Adams said. Other metals would be stolen, too, but it isn't practical. "Aluminum and copper are the ones that stand out. They are on highways," Adams said.

Source: http://www.nytimes.com/aponline/business/AP-Metal-Thefts.htm?_r=1&oref=slogin

2. *June 06, Energy Information Administration* — **Energy Information Administration: Short-Term Energy Outlook June 2006.**

The Energy Information Administration reports expecting no significant improvement in the world petroleum supply and demand balance during 2006 and 2007. While 2006 domestic production will grow with recovery from last year's hurricanes, only moderate increases in Organization of the Petroleum Exporting Countries (OPEC) and other non-OPEC production and capacity are expected. Steady and continued growth in world oil demand, only modest increases in world surplus oil production capacity, and continued risks of geopolitical instability are projected to keep crude oil prices high through 2007.

Source: <http://www.eia.doe.gov/steo>

3. *June 06, New York Times* — **New York grid could stand to lose reactors, panel says.** New York's electrical grid could get along without the Indian Point nuclear reactors, but replacing their output would be difficult and expensive, according to a report by a special committee of the National Academy of Sciences. The report said electric demand is growing so fast in the region that even if the reactors stay in operation, simply keeping the lights on in peak summer periods will be a challenge in coming years. The report stated: "While the committee is optimistic that technical solutions do exist for the replacement of Indian Point, it is considerably less confident that the necessary political, regulatory, financial and institutional mechanisms are in place to facilitate the timely implementation of these replacement options." At the moment, building any power plant in New York State is difficult, the report said, because a law that governed environmental reviews and permits for new plants was allowed to expire in 2003. The amount of generating capacity under construction now is inadequate to meet peak demand in 2009, and the shortfall would be far larger if Indian Point closes, it said.

Source: <http://www.nytimes.com/2006/06/06/nyregion/06cnd-nuke.html>

4. *June 05, Chattanooga (TN)* — **TVA, other agencies to conduct nuclear exercise.** The Tennessee Valley Authority (TVA) and other federal, state, and local agencies will conduct a regularly scheduled emergency preparedness exercise for Watts Bar Nuclear Plant on Wednesday, June 7. The exercise will involve about 1,000 TVA and state of Tennessee employees and emergency responders in McMinn, Meigs, Rhea, and Roane counties. Residents of these counties may see radiological monitoring teams or other responders in action as part of the exercise and may hear on-site and off-site sirens sound. Representatives of the U.S. Department of Homeland Security and the Nuclear Regulatory Commission will evaluate responders on the appropriateness of their actions to ensure the health and safety of the public. This emergency exercise is part of a long-term drill and exercise program. Utilities operating nuclear power plants are required by the NRC to conduct emergency exercises annually. Every two years, the Department of Homeland Security evaluates the readiness of state and local agencies to protect public health and safety.

Source: http://www.chattanooga.com/articles/article_87029.asp

[\[Return to top\]](#)

Chemical Industry and Hazardous Materials Sector

5. *June 06, Pensacola News Journal (FL)* — **Gas leak at industrial plant kills employee.** One worker died and another was treated at a hospital after the accidental release of a highly toxic gas at a Santa Rosa County, FL, industrial plant Monday, June 5. Law enforcement officials said the incident occurred at the Blackjack Creek Treating Facility on Cobbtown Road in Allentown. Investigators are trying to determine how hydrogen sulfide, an extremely toxic chemical created in the process of making crude oil, leaked into the air. The leak was confined to the plant site, and no evacuation order was issued.

Source: <http://www.pensacolanejournal.com/apps/pbcs.dll/article?AI D=/20060606/NEWS01/606060315/1006>

6. *June 06, Bay City News (CA)* — **Officials in California investigate chemical release.** A half-mile shelter-in-place has been lifted following a chemical release from a tanker in East Palo Alto, CA. The chemical release took place Monday night, June 5, at Romic Chemical. A tanker on the property, but not associated with the chemical facility itself, vented its vapor product, made up of 15 different chemicals, creating a "very large plume" that prompted officials to call for a shelter-in-place.

Source: <http://www.mercurynews.com/mld/mercurynews/news/14752600.htm>

[\[Return to top\]](#)

Defense Industrial Base Sector

Nothing to report.

[\[Return to top\]](#)

Banking and Finance Sector

7. *June 06, Associated Press* — **Computers stolen in Ohio with 72,000 Medicaid subscribers' personal info.** Laptop computers with personal information on 72,000 Ohio Medicaid recipients were stolen from a private managed care agency in Ohio. Officials with Buckeye Community Health Plan notified authorities that four computers were stolen from their Columbus office. Two contained demographic information, including names, addresses, and Social Security numbers for all of the agency's 72,000 subscribers in Lucas, Summit, and Stark counties, as well as medical information on 13,000 consumers in Stark County. The company said it will mail out notices to all customers, outlining steps they can take to protect themselves against identity theft. Accessing the computers requires a password, but the files themselves are not password protected, said Jon Allen of Job and Family Services. Robert Schenk of Buckeye Community Health Plan said the company believes the thieves wanted the computers, not the information they contained. Police are investigating.

Source: <http://www.insurancejournal.com/news/midwest/2006/06/06/69179.htm>

8. *June 05, Consumer Affairs* — **Many scammers no longer accept credit cards; they'd rather get direct access to bank accounts.** Scammers have a number of ways to steal from you, but the credit card is losing popularity among the criminal class. As consumers have become more protective of their credit card information in recent years and as credit card companies have improved security, scammers have had to look for alternate ways to commit their crimes. Since consumers are protected from large unauthorized charges, banks are more likely to go after credit card thieves. Today, a scammer would rather get access to a bank account number than a credit card. With the bank account number, a scammer can access an account and take all the money in it.

Source: http://www.consumeraffairs.com/news04/2006/06/scammers_credit_cards.html

[\[Return to top\]](#)

Transportation and Border Security Sector

9. *June 06, Agence France-Presse* — **China Southern to join SkyTeam alliance next year.** China's biggest airline, China Southern, is to become a member of the global airline alliance SkyTeam next year, the 10 members of the alliance announced on Friday, June 2. "China Southern is taking the steps to join the alliance and will confirm again in the course of June its firm desire to join SkyTeam in the course of the year 2007," the chairman of Air France-KLM, Jean-Cyril Spinetta told a news conference. The inclusion of China Southern, which transported 44.1 million passengers in 2005, is expected to help other airlines in the SkyTeam alliance gain access to the fast-growing Chinese market for air travel. SkyTeam groups 10 carriers, including Air France-KLM, Continental, and Delta, which cooperate on reservations, connections, check-in, frequent-flier miles and other services for travellers.

Source: http://www.usatoday.com/travel/flights/2006-06-05-skyteam-chinasouthern_x.htm

10. *June 06, USA TODAY* — **Planes using turned-up wing tips.** High jet fuel prices are triggering newfound interest among airlines in winglets. Aviation Partners Boeing (APB), the largest independent winglet manufacturer in the world, says it will deliver 530 sets to commercial airlines in 2006, a 51 percent increase from last year. In 2005, APB, a joint venture between Boeing and Aviation Partners, received about 780 new orders, and it expects to equal or exceed the total this year, says Patrick LaMoria, an APB sales executive. Winglets, an upturned extension of airplane wings that reduces drag and improves fuel efficiency, have been around for many years in private and military jets. But they had been historically too expensive for commercial airlines, says Mark Moran, a Continental Airlines executive. That changed when jet fuel prices began to rise near the end of 2003. The persistent high fuel prices since Hurricane Katrina have sustained airline interest in spending the extra money on winglets to cut fuel use. Continental has installed 136 sets and plans to install up to 127 more. APB's list price for a set of winglets for a Boeing 737 is \$725,000. APB says fuel savings range from three percent to five percent.

Source: http://www.usatoday.com/travel/flights/2006-06-05-winglets-travel_x.htm

11. *June 06, Houston Chronicle* — **Guard troops to arrive at Texas border by July.** About 500 National Guard troops will head for Texas' border with Mexico by July 1, in the first phase of the Bush administration's plan to buttress the U.S. Border Patrol, officials said Monday, June 5. Decisions on where to deploy Guard troops, and which troops to use, were being worked out in

meetings in Arizona and Washington on Monday under the program called Operation Jump Start. But the first 800 troops would arrive in the four border states by June 15, Lt. Gen. Steven Blum of the National Guard vowed, and the numbers will grow to 2,500 by the end of the month. Of those, about 500 troops will be sent to Texas, mostly in the El Paso area, Blum said. Texas Governor Rick Perry was hoping to use Texas National Guard soldiers and airmen to fill the missions within state borders, spokesperson Kathy Walt said. Texas Guard officials were among those meeting in Tucson, AZ, to work out details of exactly how to use the initial phase of Guard troops in California, Arizona, New Mexico, and Texas.

Source: <http://www.chron.com/disp/story.mpl/nation/3939846.html>

12. *June 06, Washington Business Journal* — **Amtrak begins Amtrak Mobile.** Amtrak says about 30,000 business travelers a day ride its trains between Washington and New York and Boston. Now they can use their PDAs to access Amtrak's Website. The new service, called Amtrak Mobile, can be accessed with a Blackberry, Treo, Pocket PC, or any Web-enabled cell phone, Amtrak says. The service can access reservations, cancellations, travel status, and schedules. Amtrak says currently no airline service offers access to as many functions as Amtrak Mobile. And the service directly accesses Amtrak's main reservations Website.

Source: <http://phoenix.bizjournals.com/washington/stories/2006/06/05/daily5.html>

13. *June 06, Washington Times* — **Airlines jettison paper tickets to save money.** Traditional airline tickets are targeted to disappear completely by the end of 2007, according to the International Air Transport Association (IATA), which represents 265 airlines worldwide. Currently, nearly half of all airline tickets are issued electronically. The association estimates the phase out could save more than \$3 billion in printing and processing costs, as the price of issuing an electronic ticket is \$1, compared with \$10 for a paper ticket. The IATA has set a goal of 70 percent of tickets to be issued electronically by the end of this year, Chairman Robert Milton told an audience at the group's annual meeting in Paris. "It's just a convenience factor," said Delta Air Lines spokesperson Gina Laughlin. "You don't have to worry about carrying something in your pocket and losing the tickets." Still, there is some reluctance among passengers to sacrifice traditional tickets and place their trust in a computer system.

Source: <http://www.washtimes.com/business/20060605-114856-3500r.htm>

14. *June 05, Associated Press* — **Fighter jets force plane to land.** No charges will be filed against a pilot who flew a small airplane into restricted airspace near Washington, DC, on Monday evening, June 5. The Federal Aviation Administration says the single-engine Cessna-182 was intercepted by two F-16s scrambled from Andrews Air Force Base 22 miles northeast of Reagan National Airport. The two jets escorted the smaller plane to the airport in Gaithersburg, MD, where it landed just after 7:00 pm EDT. The pilot was interviewed there by the Secret Service, which determined that the pilot accidentally flew into the restricted airspace.

Source: http://www.wusatv9.com/news/news_article.aspx?storyid=49954

[[Return to top](#)]

Postal and Shipping Sector

Nothing to report.

[[Return to top](#)]

Agriculture Sector

15. *June 06, Agricultural Research Service* — **Sentry lab searches for threats to U.S. grains.** For more than 80 years, the Agricultural Research Service (ARS) Cereal Disease Laboratory has been a sentry for wheat, barley and oat diseases. In addition to monitoring for wheat scab, leaf rust, stripe rust and Asian soybean rust. ARS scientists are also monitoring for a new strain of stem rust from Africa. The new strain of the wheat stem rust, Ug99, has emerged as an international threat to wheat and barley. Rusts are fungal diseases whose spores are spread by the wind. Ug99 first surfaced in Uganda in 1999. It is now in Kenya and Ethiopia. ARS is leading a search for resistance to Ug99 in U.S. wheat, as part of a new Global Rust Initiative. Eighty percent of the hard red spring wheat grown in the U.S. Northern Plains has no resistance to this new race of stem rust. If Ug99 does reach this country, it will likely first be spotted by the Cereal Disease Laboratory scientists who monitor fields from south to north annually. ARS geneticist Les Szabo is working on developing molecular tools to detect Ug99. This test would detect spores in rain samples.

Source: <http://www.ars.usda.gov/News/docs.htm?docid=1261>

16. *June 06, AgProfessional* — **Counterfeit iron injection product linked to death of Canadian horse.** A Canadian biopharmaceutical company has issued a warning that a counterfeit version of its iron–sucrose injection may be associated with the death of a horse in Ontario, Canada. Bioniche Life Sciences Inc. said its product, Hippiron(TM) 1000, fully complies with regulatory standards and is safe for use as recommended. Bioniche sells this injectable iron–sucrose product exclusively to veterinarians, and it is the only licensed product of its kind available for veterinary use in Canada. At least one horse in Ontario has died and two more have had serious reactions following the administration of a counterfeit product sourced from a feed store. Health Canada's Veterinary Drugs Directorate and Health Products & Food Branch Inspectorate are investigating the source of the counterfeit product in order to prevent any further use in Canadian horses. Hippiron 1000 is an iron–sucrose product for horses that is administered by IV injection. It is widely used to treat iron deficiency (equine anaemia).

Source: http://www.agprofessional.com/show_story.php?id=40893

17. *June 05, U.S. Department of Agriculture* — **Documentation tools to assist producers with soybean rust prevention and control provided.** U.S. Department of Agriculture (USDA) Deputy Secretary Chuck Conner announced Monday, June 5, the launch of the Risk Management Agency's (RMA) Good Farming Practices Documentation Tool. This tool enables farmers to quickly and accurately record actions taken to prevent and treat any outbreak of soybean rust. The documentation tool is part of USDA's Pest Information Platform for Extension and Education (PIPE). PIPE is an online, real–time observation and forecasting system that allows growers to access the latest information about which counties have confirmed the disease and/or insect pest outbreaks. State extension specialists provide frequently updated commentaries discussing the immediate and future risks and control guidelines. Growers can sign up for email notification when risks change for soybean rust in their states. PIPE tracks the spread of soybean rust as well as soybean aphids in soybeans and dry beans. The PIPE network grew out of USDA's Soybean Rust Information System. That system is estimated to have helped increase U.S. soybean growers' profits by as much as \$299 million in 2005, according to a study by the Economic Research Service.

Good Farming Practices Documentation Tool: <http://www.sbrusa.net>
Source: http://www.usda.gov/wps/portal/!ut/p/s.7_0_A/7_0_1OB?contentonly=true&contentid=2006/06/0188.xml

[\[Return to top\]](#)

Food Sector

18. *June 02, ABC (Australia)* — **Millions of cakes destroyed after tampering incidents.** The company at the center of a major food tampering incident has begun destroying millions of dollars worth of its bakery products. George Weston Foods announced the voluntary recall after foreign objects, including a razor blade and a sewing needle, were found in its Top Taste cakes in Queensland, Victoria and Tasmania, Australia. Spokesperson Peter Schutz says more than four million cakes made at the company's Brisbane plant will be buried at several disposal sites. He says the cakes will be buried at a secure site. Police are still investigating the tampering incidents.

Source: <http://www.abc.net.au/news/items/200606/1654265.htm?queensland>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

19. *June 06, Agence France–Presse* — **Asia–Pacific nations to test bird flu pandemic response.**

Major countries in the Asia–Pacific region will Wednesday, June 7, take part in an exercise to test their response to an outbreak of a bird flu pandemic. The exercise, which will include the 21 Asia–Pacific Economic Cooperation (APEC) members, will be coordinated by Australia. APEC Pandemic Response Exercise 2006 will force senior officials from relevant agencies from around the region to make real–time decisions to manage an outbreak. It will involve a hypothetical scenario in which the bird flu virus has mutated into a form which allows human–to–human transmission and has escalated to a pandemic level. Neil Head, project director with Emergency Management Australia, which will coordinate the exercise, said the simulation would test communication links between the 21 APEC economies. Several APEC nations, including Indonesia and Vietnam, have suffered deadly bird flu outbreaks among humans. APEC also includes Australia, Brunei, Canada, Chile, China, Hong Kong, Japan, South Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Singapore, Russia, Taiwan, Thailand and the United States.

Source: http://news.yahoo.com/s/afp/20060606/hl_afp/healthfluaustralia_060606105951:ylt=Ahd6Yqooxv1Ld753mLIbmWaJOrgF:ylu=X3oDMTA5aHJvMDdwBHNIYwN5bmNhdA--

20.

June 06, Reuters — **Namibia confirms seven dead in polio outbreak.** Namibia's first suspected polio outbreak in more than a decade has killed seven people since early May, spurring the southern African nation to launch a mass vaccination program, officials said on Tuesday, June 6. Specimens collected from 11 patients were sent to South African laboratories for investigation last week, and state health officials said five of the specimens were identified as polio. Final confirmation was expected later this week. Namibia was considered polio-free in the early 1990s but saw an outbreak of 53 cases of the disease in 1993, spurring another immunization drive. Namibia's last reported polio case was in 1995, according to the World Health Organization (WHO). "We are certainly concerned ... there is a very important outbreak of paralytic disease that could well represent further spread (of polio)," said Bruce Aylward, coordinator of WHO's polio initiative. Aylward said further tests could indicate where the virus had spread from, adding that neighboring Angola was the most likely source given that there was an outbreak there last year.

Global Polio Eradication Initiative: <http://www.polioeradication.org/>

Source: http://za.today.reuters.com/news/NewsArticle.aspx?type=topNews&storyID=2006-06-06T144219Z_01_ALL646860_RTRIDST_0_OZATP-HEALTH-NAMIBIA-POLIO-20060606.XML

[\[Return to top\]](#)

Government Sector

21. *June 06, Associated Press* — **President signs disaster declaration for California following spring storms.** President Bush on Monday, June 5, declared a federal disaster in 17 Northern California counties struck by storms and flooding in March and April. The spring storms left many reservoirs in California's Central Valley at full capacity, and triggered scattered levee breaks. It washed out roads, deposited tons of debris, and forced hundreds of residents from their homes. Governor Arnold Schwarzenegger declared state disasters in more than three-dozen California counties between January and April. He also asked Bush for an unusual pre-emptive federal disaster declaration covering the state's fragile levee system.

Source: <http://www.signonsandiego.com/news/state/20060605-1714-ca-bush-californiaflooding.html>

[\[Return to top\]](#)

Emergency Services Sector

22. *June 06, Muscatine Journal (IA)* — **Emergency dispatchers in Iowa make temporary move.** As mudjacking work began at the Muscatine, IA, Public Safety Building, uncertainty about how loud the noise would be and how long the construction project would last forced Muscatine Joint Communications Center (MUSCOM) director Joe McCarville, to temporarily move part of the center to the county's recently acquired emergency management trailer. Under the temporary dispatch setup, McCarville said computer and telephone technicians moved MUSCOM's 911 telephone system, business telephone lines, a computer-aided dispatch terminal and other miscellaneous equipment to the trailer. Despite the inconvenience, the temporary move may provide some benefit for MUSCOM and other local public safety

agencies, McCarville said. "We may need to use the trailer as a dispatch center during an emergency, so it was important to learn how fast we could convert it," he said. "Now we know how much time and work it takes."

Source: <http://www.muscatinejournal.com/articles/2006/06/01/news/doc447f048509392720099419.txt>

23. *June 06, Austin American–Statesman (TX)* — State's strategy to evacuate Texans released.

The Texas hurricane evacuation and sheltering plan shows significant improvements since Hurricane Rita last fall exposed flaws, but nearly a week into hurricane season, a great deal of uncertainty remains, several officials from across Texas said. The state's 157–page plan was posted online late Friday, June 2, the day after the Atlantic hurricane season began. Some local emergency management officials said Monday, June 5, that they did not know the plan was ready. But several who had seen it said the plan sufficiently addresses some of the most crucial concerns from last year, including traffic management, fuel availability along evacuation routes and the evacuation of people who can't move themselves. The plan includes several new components, such as "comfort stations" that would provide food, water and medical assistance along evacuation routes and a point–to–point system that would pair coastal cities with inland cities for special needs evacuations.

Texas Hurricane and Mass Care Plan:

ftp://ftp.txdps.state.tx.us/dem/plan_state/hurr_evac_shelter_state_plan.pdf

Additional evacuation information:

[#hurrevac](http://www.txdps.state.tx.us/dem/pages/downloadableforms.htm)

Source: <http://www.statesman.com/news/content/news/stories/local/06/6hurricane.html>

24. *June 05, University of Iowa FYI* — Tornado puts University of Iowa's emergency response plan to the test.

When a tornado ripped through Iowa City on April 13, it wasn't a complete disaster. The tornado put the University of Iowa's (UI) Critical Incident Management Plan to a severe test that gave Chuck Green, director of the UI Public Safety, and others their best chance yet to see how well the plan protects the UI community. "It was managed chaos...But the plan worked. Communication went well — those of us charged with responding knew what to do and could relay instructions and information." The plan covers a lot of ground. It focuses on specific types of crises: bomb threats, civil protests, explosions, fire, flood, hazardous materials incidents, infrastructure failure, snow and ice storms, tornadoes, and violence. But the plan did not prepare Green and his officers for the crowds who filled the streets shortly after the tornado struck. Green would like to step up safety education at the start of the tornado season, as well as research new advanced warning systems, including paging or calling systems that would send an alert to all 125 campus buildings at the touch of a button from the public safety dispatcher.

The Critical Incident Management Plan: <http://www.uiowa.edu/~our/opmanual/v/16.htm>

Source: http://www.uiowa.edu/~fyi/issues/issues2006_v43/06052006/cim_p.html

[[Return to top](#)]

Information Technology and Telecommunications Sector

25. *June 06, Reuters* — IBM to pour \$6 billion into India. IBM plans to invest nearly \$6 billion in India over three years, underscoring the country's ever-increasing importance as a global hub for IT outsourcing and expertise. IBM, the world's largest computer services company, said

Tuesday, June 6, that it plans to expand its services, software, hardware and research businesses in India, where it already is the largest multinational company with 43,000 employees in 14 cities, up from 4,900 in 2002. The deal, almost triple the \$2 billion that IBM has already invested in India over the past three years, is the biggest investment by a multinational firm in India in recent years.

Source: http://news.com.com/IBM+to+pour+6+billion+into+India/2100-1014_3-6080346.html?tag=nefd.top

- 26. June 05, Security Focus — Microsoft Internet Explorer frameset denial-of-service vulnerability.** Microsoft Internet Explorer is affected by a denial-of-service vulnerability. Analysis: This issue arises because the application fails to handle exceptional conditions in a proper manner. An attacker may exploit this issue by enticing a user to visit a malicious site and then to click anywhere on the page. This results in a denial-of-service condition in the application.

For a complete list of vulnerable products: <http://www.securityfocus.com/bid/18277/info>

Solution: This issue reportedly does not affect Internet Explorer version 7 beta 2. Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Source: <http://www.securityfocus.com/bid/18277/references>

- 27. June 05, Tech Web — OpenOffice.org denies macro exploit a problem.** OpenOffice.org, the open-source project that produces an alternative to Microsoft's Office suite, said it won't patch its software against a recently launched macro threat. In a statement, the group also disputes applying the label "virus" to Stardust, the proof-of-concept exploit discovered last week by Kaspersky Labs. "The 'proof-of-concept macro virus' showed that it is possible to write a simple 'virus-like' program using OpenOffice.org's macro language," read the statement. "This is a known risk with any capable macro language. To mitigate against this risk, by default OpenOffice.org detects if a document contains macros, displays a warning, and will only run the macro if the user specifically agrees."

Source: <http://www.informationweek.com/news/showArticle.jhtml;jsessioid=2UV2DAIAPNQBWQSNDBOCKICCCJUMEKJVN?articleID=188701739>

- 28. June 05, Tech Web — Microsoft adds new help on Word zero-day.** Microsoft revised a security advisory targeting an in-the-wild exploit of Word XP and Word 2003 to clarify a work-around for enterprises, repeated that it was on track to deliver a fix Tuesday, June 13, and offered up another tactic to protect users. The advisory, which was revised Friday, June 2, now includes more detail about how corporations can defend themselves by using group policies to force Word into running in "Safe Mode."

Microsoft Security Advisory: <http://www.microsoft.com/technet/security/advisory/919637.mspx>

Source: <http://www.informationweek.com/security/showArticle.jhtml?articleID=188701743&subSection=Viruses+and+Patches>

- 29. June 05, USA Today — Cybercrime spurs college courses in digital forensics.** One of the hottest new courses on U.S. college campuses is a direct result of cybercrime. Classes in digital forensics — the collection, examination and presentation of digitally stored evidence in criminal and civil investigations — are cropping up as fast as the hackers and viruses that spawn them. About 100 colleges and universities offer undergraduate and graduate courses in

digital forensics, with a few offering majors. Students learn where to find digital evidence and handle it without contaminating it. Once preserved, students are shown how to examine evidence and present it clearly during court testimony.

Source: http://www.usatoday.com/tech/news/techinnovations/2006-06-05-digital-forensics_x.htm?POE=TECISVA

30. June 05, Government Computer News — Spyware infections spreading, security expert says.

Spyware programs are increasing in number and growing in sophistication to avoid detection, making it harder to guard against infections and more costly to repair their damage, according to a security expert. Gerhard Eschelbeck, chief technology officer for Webroot Software Inc. told the audience at Techno Security 2006 that through the first quarter of this year, his company has identified approximately 427,000 Websites that host spyware. In addition, “there are at least 10 variants for each spyware program identified,” Eschelbeck said, to make them stealthier and harder to detect.

Source: http://www.gcn.com/online/vol1_no1/40943-1.html

Internet Alert Dashboard

DHS/US-CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US-CERT Operations Center Synopsis: US-CERT is aware of a buffer overflow vulnerability in Symantec Client Security and Symantec Antivirus Corporate Edition. Successful exploitation may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges. We are not aware of any public exploits at this time. For more information please review the following:

VU#404910 – Symantec products vulnerable to buffer overflow:

<http://www.kb.cert.org/vuls/id/4049100>

Symantec Advisory SYM06-010 – Symantec Client Security and Symantec AntiVirus Elevation of Privilege:

<http://securityresponse.symantec.com/avcenter/security/Content/2006.05.25.html>

US-CERT will advise as more information becomes available.

Active Exploitation of a Vulnerability in Microsoft Word

US-CERT is aware of an increase in activity attempting to exploit a vulnerability in Microsoft Word. The exploit is disguised as an email attachment containing a Microsoft Word document. When the document is opened, malicious code is installed on the user's machine. More information about the reported vulnerability can be found in the following:

TRA06-139A – Microsoft Word Vulnerability:
<http://www.us-cert.gov/cas/techalerts/TA06-139A.html>

VU#446012 – Microsoft Word buffer overflow:
<http://www.kb.cert.org/vuls/id/446012>

Review the workarounds described in Microsoft Security Advisory 919637:
<http://www.microsoft.com/technet/security/advisory/919637.mspx>

US-CERT strongly encourages users not to open unfamiliar or unexpected email attachments, even if sent by a known and trusted source. US-CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US-CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US-CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US-CERT.
http://www.us-cert.gov/nav/report_phishing.html

Non-federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. <http://onguardonline.gov/phishing.html>

Current Port Attacks

Top 10 Target Ports	1026 (win-rpc), 6881 (bittorrent), 4672 (eMule), 445 (microsoft-ds), 50497 (---), 25 (smtp), 54856 (---), 20282 (---), 113 (auth), 80 (www) Source: http://isc.incidents.org/top10.html ; Internet Storm Center
----------------------------	--

To report cyber infrastructure incidents or to request information, please contact US-CERT at soc@us-cert.gov or visit their Website: www.us-cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: <https://www.it-isac.org/>.

[\[Return to top\]](#)

Commercial Facilities/Real Estate, Monument & Icons Sector

Nothing to report.

[\[Return to top\]](#)

General Sector

Nothing to report.

[\[Return to top\]](#)

DHS Daily Open Source Infrastructure Report Contact Information

[DHS Daily Open Source Infrastructure Reports](#) – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: <http://www.dhs.gov/iaipdailyreport>

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644.

Subscription and Distribution Information:

Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983–3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.

To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us-cert.gov or visit their Web page at www.us-cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.